

Author Index for Volume 17

- Benton, J.R. 389
Bequai, A. 19, 22, 293, 381, 579, 667
Bontchev, V. 69
Borcherding, B. 447
Borcherding, M. 447

Caminada, M. et al 417
Chor, L.P. et al 725
Coffey, T. 253
Cohen, F. 483
Cohen, F. et al 211
Crocker, N. 42

Dawson, E.P. 177

Eloff, J.H.P. 233, 347, 683

Finne, T. 303, 397
Ford, R. 575

Geldenhuis, J.H.S. 337
Ghosh, S. 527
Gordon, S. 586
Gustafson, H.M. 177

Hinde, S. 31, 115, 207, 299, 385, 475, 583, 671

Kagan, A. 589
Kapidzic, N. 507
Kovacich, G. 129, 600

Labuschagne, L. 347
Lau, O. 119
Lee, T-C 543
Lichtenstein, S. 143
Lin, C-H 543

Maddison, N. 201
Matyas, M. et al 265
Moulton, M. 137

Nacht, M. 54
Newe, T. 253

Osborne, K. 34
Ozier, W. 14

Peyravian, M. et al 171
Post, G. 589
Pounder, C. 27, 124, 308, 392, 479

Ratnasingham, P. 313

Schumacher, H.J. 527
Schwartau, W. 693
Schwemmlein, J. et al 637

van der Merwe, G. 233
van der Merwe, J. 435
Venter, H.S. 683
von Solms, S.H. 337, 435

Subject Index for Volume 17

- Asymmetric key
 - reversible data mixing procedure for efficient public-key encryption 265
- ATM network
 - a fundamental framework for network security towards enabling security on demand in an ATM network 527
- Auditing
 - auditing and the IT security function 34
- Authentication
 - efficient and trustworthy key distribution in webs of trust 447
- Authorization applet
 - collecting security baggage on the Internet 337
- Baggage
 - collecting security baggage on the Internet 337
- Birthday paradox
 - a method for measuring entropy of symmetric cipher key generators 177
- Black-box analysis
 - a method for measuring entropy of symmetric cipher key generators 177
- Block cipher
 - a confused document encrypting scheme and its implementation 543
- CA-ACF2/MVS
 - key concerns in a review of CA-ACF2/MVS 42
- Certificate Management System
 - creating security applications based on the global Certificate Management System 507
- Character position table
 - a confused document encrypting scheme and its implementation 543
- Cheating text
 - a confused document encrypting scheme and its implementation 543
- Code analysis
 - software source code, visual risk analysis: an example 233
- Compsec '98
 - time, history and war: a personal voyage through Compsec '98 671
- Computer arithmetic
 - RNS-modulo reduction upon a restricted base value set and its applicability to RSA cryptography 637
- Computer crime
 - Internet security incidents, a survey within Dutch organizations 417
- Corporate governance
 - corporate governance and disasters 583
- Cryptography
 - on probabilities of hash value matches 171
 - RNS-modulo reduction upon a restricted base value set and its applicability to RSA cryptography 637
- Cyber-crime
 - a guide to cyber-crime investigations 579
- Cyberspace
 - balancing legal concerns over crime and security in cyberspace 293
 - employee abuses in cyberspace: management's legal quagmire 667
- Cyber wars
 - cyber wars and other threats 115
- Data mixing
 - reversible data mixing procedure for efficient public-key encryption 265
- Data protection
 - security and the new data protection law 124
 - the Annual Report of the UK Data Protection Register 479

- Databases
on probabilities of hash value matches 171
- Datagrams
the use of real-time risk analysis to enable dynamic activation of countermeasures 347
- Decision-making
the three categories of decision-making and information security 397
- DES
a confused document encrypting scheme and its implementation 543
- Digital signatures
further developments in the field of encryption and digital signatures 308
realisation of a minimum-knowledge identification and signature scheme 253
- Disasters
corporate governance and disasters 583
hot water, icebergs and others 31
- Distributed objects
electronic commerce with secure intelligent trade agents 435
- Distributed resources allocation
a fundamental framework for network security towards enabling security on demand in an ATM network 527
- Document protection
a confused document encrypting scheme and its implementation 543
- EDI
EDI security: the influences of trust on EDI risks 313
- Electronic commerce
electronic commerce with secure intelligent trade agents 435
privacy and security - the drivers for growth of E-commerce 475
- Electronic communications (E-Comm)
reducing charges of E-Comm harassment 137
- Employees
employee abuses in cyberspace: management's legal quagmire 667
- Encryption
further developments in the field of encryption and digital signatures 308
reversible data mixing procedure for efficient public-key encryption 265
- Entropy
a method for measuring entropy of symmetric cipher key generators 177
- European Commission
European Commission takes action to secure the Internet 392
- Fiat-Shamir
realisation of a minimum-knowledge identification and signature scheme 253
- Firewalls
spectrum of modern firewalls 54
the use of real-time risk analysis to enable dynamic activation of countermeasures 347
- Fuzzy logic
the use of real-time risk analysis to enable dynamic activation of countermeasures 347
- Generally Accepted System Security Principles (GSSP) preface/overview 14
- Geometric approach
a geometric approach for shared secrets, a refinement 725
- Global risk value
the use of real-time risk analysis to enable dynamic activation of countermeasures 347
- GSSP
GSSP preface/overview 14
- Hackers
Internet security incidents, a survey within Dutch organizations 417
- Hash functions
on probabilities of hash value matches 171
reversible data mixing procedure for efficient public-key encryption 265
- Hashing algorithm
realisation of a minimum-knowledge identification and signature scheme 253
- Homeworking
homeworking: no longer an easy option? 27

Subject Index

IDEA

a confused document encrypting scheme and its implementation 543

Identity verification

realisation of a minimum-knowledge identification and signature scheme 253

Indexing

on probabilities of hash value matches 171

Information protection

a note on the role of deception in information protection 483

Information security

the three categories of decision-making and information security 397

Information security management

a conceptual framework for information security management 303

Information systems

cause and effect model of attacks on information systems 211

Information Systems Security Organization (ISSO)

establishing an Information Systems Security Organization (ISSO) 600

Intelligent agents

electronic commerce with secure intelligent trade agents 435

Interesting times

may you live in interesting times 575

Intermediate risk value

the use of real-time risk analysis to enable dynamic activation of countermeasures 347

Internet

collecting security baggage on the Internet 337
data packet intercepting on the Internet: how and why? 683

electronic-Internet business and security 129

European Commission takes action to secure the Internet 392

Internet risks for companies 143

Internet security incidents, a survey within Dutch organizations 417

the use of real-time risk analysis to enable dynamic activation of countermeasures 347

IT security

auditing and the IT security function 34

physical IT security 389

Java

collecting security baggage on the Internet 337

Key distribution

efficient and trustworthy key distribution in webs of trust 447

Key generation

a method for measuring entropy of symmetric cipher key generators 177

Key management

efficient and trustworthy key distribution in webs of trust 447

(k, n) threshold scheme

a geometric approach for shared secrets, a refinement 725

Long integer arithmetic

RNS-modulo reduction upon a restricted base value set and its applicability to RSA cryptography 637

Millenium

contingency planning for the Millenium 299

Minimum-knowledge

realization of a minimum-knowledge identification and signature scheme 253

Modular arithmetic

realization of a minimum-knowledge identification and signature scheme 253

Modulo reduction

RNS-modulo reduction upon a restricted base value set and its applicability to RSA cryptography 637

Multiple precision

realization of a minimum-knowledge identification and signature scheme 253

Network security

a fundamental framework for network security towards enabling security on demand in an ATM network 527

Ohta-Okamoto

realization of a minimum-knowledge identification and signature scheme 253

- Packet filtering
the use of real-time risk analysis to enable dynamic activation of countermeasures 347
- Parallel algorithms
RNS-modulo reduction upon a restricted base value set and its applicability to RSA cryptography 637
- PCM
collecting security baggage on the Internet 337
- Plaintext index file
a confused document encrypting scheme and its implementation 543
- Prime numbers
realization of a minimum-knowledge identification and signature scheme 253
- Privacy
privacy and security - the drivers for growth of E-commerce 475
- Probabilistic cryptosystem
a confused document encrypting scheme and its implementation 543
- Program visualization
software source code, visual risk analysis: an example 233
- Public key
RNS-modulo reduction upon a restricted base value set and its applicability to RSA cryptography 637
- Public key encryption
electronic commerce with secure intelligent trade agents 435
- Random numbers
realization of a minimum-knowledge identification and signature scheme 253
- Repetitions
a method for measuring entropy of symmetric cipher key generators 177
- Residue number systems
RNS-modulo reduction upon a restricted base value set and its applicability to RSA cryptography 637
- Risk analysis
Internet security incidents, a survey within Dutch organizations 417
software source code, visual risk analysis: an example 233
- the use of real-time risk analysis to enable dynamic activation of countermeasures 347
- Risks
EDI security: the influences of trust on EDI risks 313
Internet risks for companies 143
- Secret sharing
a geometric approach for shared secrets, a refinement 725
- Security
auditing and the IT security function 34
breaking the chain 586
creating security applications based on the global Certificate Management System 507
EDI security: the influences of trust on EDI risks 313
electronic-Internet business and security 129
high-tech security and the failings of President Clinton's commission on critical infrastructure protection 19
Internet security incidents, a survey within Dutch organizations 417
on probabilities of hash value matches 171
physical IT security 389
privacy and security - the drivers for growth of E-commerce 475
recent security surveys 207
security and the new data protection law 124
software source code, visual risk analysis: an example 233
the ten commandments of security 119
time-based security explained: provable security models and formulas for the practitioner and vendor 693
- Security on demand
a fundamental framework for network security towards enabling security on demand in an ATM network 527
- Smartcards
realization of a minimum-knowledge identification and signature scheme 253
- Software attacks
software source code, visual risk analysis: an example 233
- Software pirating
software pirating and management's quagmire 22
- Solar radiation
solar radiation is bad for you 385

Subject Index

- Source code
 - software source code, visual risk analysis: an example 233
- Symmetric ciphers
 - a method for measuring entropy of symmetric cipher key generators 177
- Symmetric key
 - reversible data mixing procedure for efficient public-key encryption 265
- TCP/IP
 - the use of real-time risk analysis to enable dynamic activation of countermeasures 347
- Techno-crimes
 - techno-crimes: failings of the legal edifice 381
- Threats
 - cyber wars and other threats 115
- Time-based security
 - time-based security explained: provable security models and formulas for the practitioner and vendor 693
- Transaction authorization
 - electronic commerce with secure intelligent trade agents 435
- Trojan horses
 - software source code, visual risk analysis: an example 233
- Trust
 - efficient and trustworthy key distribution in webs of trust 447
- Trusted third party
 - collecting security baggage on the Internet 337
- UK Data Protection Registrar
 - the Annual Report of the UK Data Protection Register 479
- Viruses
 - macro virus identification problems 69
 - the use and effectiveness of anti-virus software 589
- Visualization
 - software source code, visual risk analysis: an example 233
- VLSI
 - RNS-modulo reduction upon a restricted base value set and its applicability to RSA cryptography 637
- Year 2000
 - Y2000 enters the body politic 201